

Exhibit B

**UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

JANE DOE, individually and on behalf of
all others similarly situated,

Plaintiff,

vs.

LEHIGH VALLEY HEALTH NETWORK,
INC.,

Defendant.

Case No.

DECLARATION OF MARY ANN LA ROCK

I, Mary Ann La Rock, depose and state as follows:

1. I am over the age of twenty-one (21), and I am competent in all respects to make this declaration. The facts stated in this declaration are within my personal knowledge and are true.

2. I am employed by Lehigh Valley Health Network, Inc. (“LVHN”) as the Chief Compliance Officer. In this position, my responsibilities include the oversight of the healthcare regulatory environment to ensure that emerging issues are addressed by LVHN policies and procedures. I have been employed by LVHN since March 2010.

3. I have reviewed the Class Action Complaint (the “Complaint”), filed on March 13, 2023, in the lawsuit styled *Doe v. Lehigh Valley Health Network, Inc.*, No. 23-cv-1149, in the Court of Common Pleas of Lackawanna County, Pennsylvania (the “State Court

Action”), and I am familiar with the allegations therein. I make this Declaration based on personal knowledge relating to such allegations.

4. LVHN was served with the State Court Action on March 28, 2023.

5. A copy of the Complaint, as well as all other process, pleadings, and orders provided to LVHN are attached hereto as **Exhibit 1**.

6. LVHN is a corporation duly organized and validly existing under the laws of the State of Pennsylvania with its principal place of business located in Allentown, Pennsylvania. Specifically, LVHN maintains its corporate headquarters in Allentown, Pennsylvania, the majority of LVHN management works out of its Allentown, Pennsylvania offices, and LVHN maintains its books and records in Allentown, Pennsylvania.

7. The Complaint describes a security incident that LVHN discovered on or about February 6, 2023 (the “Security Incident”).

8. LVHN’s investigation into the Security Incident is ongoing, and LVHN is working to identify the universe of potentially affected individuals and data elements and to obtain contact information by which those individuals can be notified.

9. Thus far, however, LVHN has identified approximately 2,760 individuals for which clinically appropriate photographs taken during the course of their medical treatment were potentially stolen as a result of the Security Incident.

10. Based on the allegations in the Complaint, LVHN understands the plaintiff in the State Court Action to be one of those individuals.

11. Based on its investigation to date, among those 2,760 individuals are residents of the states of New York, New Jersey, Virginia, Georgia, and California.

12. There are additional individuals who had other information—but not clinically appropriate photographs—potentially stolen as a result of the Security Incident. Based on LVHN’s investigation to date, a number of these individuals reside outside the State of Pennsylvania.

13. I have also reviewed the “Motion and Incorporated Memorandum of Law in Support of Preliminary Injunction Without Hearing” filed by the plaintiff in the State Court Action on or about April 4, 2023. That motion seeks as relief an order requiring LVNH to pay a ransom demand made to LVHN by the ransomware gang known as ALPHV *aka* BlackCat (“ALPHV”).

14. The ransom demand that ALPHV made to LVHN in connection with the Security Incident was in excess of \$5 million.

[SIGNATURE ON FOLLOWING PAGE]

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

April 5, 2023
Date

Mary Ann LaRock
Mary Ann La Rock
Chief Compliance Officer

Exhibit 1

SALTZ, MONGELUZZI, & BENDESKY, P.C.

By: Simon B. Paris

Patrick Howard, Esquire (No. 88572)

One Liberty Place, 52nd Floor

1650 Market Street

Philadelphia, PA 19103

T: 215-496-8282; F: 215-754-4443

MATTER. A JURY OF TWELVE

(12) PERSONS IS DEMANDED.

MAURI B. KELLY
LACKAWANNA COUNTY

2023 MAR 13 P 2:51

CLERK OF JUDICIAL
RECORDS CIVIL DIVISION

ATTORNEYS FOR PLAINTIFF

*(Additional Counsel Listed on Signature Page)***JANE DOE,
Dunmore, PA 18512***individually and on behalf of all
others similarly situated,***Plaintiff,**

v.

**LEHIGH VALLEY HEALTH
NETWORK, INC.****1243 Cedar Crest Blvd.
Allentown, PA 18103****Defendant.****IN THE COURT OF COMMON PLEAS
OF LACKAWANNA COUNTY****Term, 2023****Case No. 23 CV 1149****CLASS ACTION****JURY TRIAL DEMANDED****NOTICE TO PLEAD****"NOTICE"**

"You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by an attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgement may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the Plaintiff. You may lose money or property or other rights important to you.

"YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.
IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH
INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A
REDUCED FEE OR NO FEE.

LACKAWANNA COUNTY BAR ASSOCIATION
LAWYER REFERRAL and INFORMATION SERVICE
200 North River Street
Wilkes-Barre, PA 18711
(570) 822-6029

"AVISO"

"Le han demandado en corte. Si usted quiere defenderse contra las demandas nombradas en las páginas siguientes, llene veinte (20) días, a partir de recibir esta demanda y la notificación para entablar personalmente o por un abogado una comparecencia escrita y también para entablar con la corte en forma escrita sus defensas y objeciones a las demandas contra usted. Sea avisado que si usted no se defiende, el caso puede continuar sin usted y la corte puede incorporar un juicio contra usted sin previo aviso para conseguir el dinero demandado en el pleito o para conseguir cualquier otra demanda o alivio solicitados por el demandante. Usted puede perder dinero o propiedad u otros derechos importantes para usted.

USTED DEBE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE ABOGADO (O NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO), VAYA EN PERSONA O LLAME POR TELEFONO LA OFICINA NOMBRADA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL. ESTA OFICINA PUEDE PROPORCIONARLE LA INFORMACION SOBRE CONTRATAR A UN ABOGADO.

SI USTED NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO, ESTA OFICINA PUEDE PROPORCIONARLE INFORMACION SOBRE AGENCIAS QUE OFRECEN SERVICIOS LEGALES A PERSONAS QUE CUMPLEN LOS REQUISITOS PARA UN HONORARIO REDUCIDO O NINGUN HONORARIO.

ASOCIACION DE LICENCIADOS DE LUZERNE
SERVICO DE REFERENCIA E INFORMACION LEGAL
200 North River Street
Wilkes-Barre, Pennsylvania 18711
(570) 822-6029

CLASS ACTION COMPLAINT

MAURI B. KELLY
LACKAWANNA COUNTY

Plaintiff, Jane Doe ("Plaintiff"), by and through her attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, files this complaint against Defendant, Lehigh Valley Health Network, Inc. ("LVHN") and alleges the following:

NATURE OF THE ACTION

1. On February 6, 2023, Defendant LVHN suffered a data breach. In general, data breaches are serious as they result in disclosure personally identifiable information ("PII") and protected health information ("PHI"), including one or more of the following: address, email address, date of birth, Social Security number, passport information, driver's license number / State ID number, health insurance provider, medical diagnosis/medical treatment information, medications, lab results, and nude photographs (collectively, "Sensitive Information").

2. This Data Breach, however, was far more consequential. Cancer patients receiving treatment were photographed in the nude—often unbeknownst to the patients themselves—and those images were stored on LVHN's network. Those images were subsequently stolen by the hackers as part of the Data Breach.

3. LVHN was told by the hackers that they had these images and if LVHN refused to pay their ransom demand, the hackers would release these sensitive images publicly. LVHN needed to act with serious consideration of the consequences that would befall these patients if those images were released on the internet where they can stay forever. LVHN made the knowing, reckless, and willful, decision to let the hackers post the nude images of Plaintiff and others on the internet.

4. Indeed, while LVHN is publicly patting itself on the back for standing-up to these hackers and refusing to meet their ransom demands, they are consciously and intentionally ignoring the real victims: Plaintiff and the Class. Rather than act in their patients' best interest, LVHN put its own financial considerations first. LVHN must be held to account for the embarrassment and humiliation it has caused Plaintiff and the Class.

5. To obtain medical treatment, Plaintiff, and other patients of LVHN, entrusted and provided LVHN an extensive amount of highly sensitive and privileged PII. Previously unknown, LVHN also maintains screenshots of patients receiving treatment for cancer in various forms of undress. LVHN referred to these photos as "clinically appropriate photographs of cancer patients receiving radiation oncology treatment[.]"

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and members of the proposed Class's Sensitive Information, LVHN assumed legal and equitable duties to those individuals.

7. Plaintiff and members of the proposed Class are victims of LVHN's negligent and/or careless acts and omissions and the failure to protect the Sensitive Information of LVHN's current and former patients.

8. As a result of LVHN's conduct, Plaintiff and the Class have suffered embarrassment and humiliation by having previously unknown nude images of themselves receiving cancer treatment posted on the internet. Adding insult to injury, Plaintiff and the Class will also have to undertake and incur out-of-pocket, expensive, and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their financial well-being. Indeed, Plaintiff, herself, has already placed fraud alerts on her accounts with credit reporting agencies, she has notified multiple financial institutions about the breach, she is also closely monitoring her

credit reports and accounts for unauthorized activity. All due to LVHN's failure to adequately maintain her Sensitive Information.

9. Plaintiff brings this class action against LVHN for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used in its ordinary course of business. Plaintiff and the putative Class seek remedies including damages, reimbursement of out-of-pocket-costs, and equitable and injunctive relief, including improvements to LVHN's data security systems, future annual audits, and identity protection services.

PARTIES

10. Plaintiff, Jane Doe, is a resident of Dunmore and citizen of Pennsylvania. Plaintiff was informed by LVHN that her Sensitive Information was compromised in the Data Breach and that nude images of her during breast cancer treatment were posted on the dark web.

11. Defendant Lehigh Valley Health Network, Inc., is a corporation organized under the laws of Pennsylvania and maintains its principal place of business at 1243 Cedar Crest Blvd., Allentown, PA 18103.

12. All of Plaintiff's claims stated herein are asserted against LVHN and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over this action pursuant to 42 Pa. C.S.A. § 931.

14. The Court has personal jurisdiction over LVHN pursuant to 42 Pa. C.S.A. § 5301(2).

15. Venue in Lackawanna County is proper pursuant to Pa. R. Civ. P. No. 2179(a) because *inter alia*, the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from Lackawanna County; LVHN transacts substantial business and has agents in Lackawanna County; a substantial part of the conduct giving rise to Plaintiff's claims occurred in Lackawanna County; and because Plaintiff resides in Lackawanna County.

FACTUAL BACKGROUND

A. Background

16. LVHN is comprised of 13 hospital campuses; 28 health centers; 20 ExpressCARE locations, and numerous physician practices, pharmacy, imaging, home health, rehabilitation, and lab services in 10 eastern Pennsylvania counties.

17. In January 2022, LVHN acquired Delta Medix, a Scranton based multispecialty group that performs more than 17,000 surgeries a year. Delta Medix added 20 providers to LVHN who specialize in urology, general surgery, cancer care and vascular surgery.

18. To obtain healthcare and related services, patients, like Plaintiff and the Class, must provide LVHN with highly sensitive information, including PHI, PII, or both. LVHN then compiles, stores, and maintains the highly sensitive PII and PHI. LVHN serves thousands of individuals per year indicating it has created and maintains a massive repository of Sensitive Information, acting as a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.

19. LVHN has a "Notice of Privacy Practices" posted on its website.¹ In it, LVHN claims that it understands that "medical information is personal" and that LVHN is committed to

¹ <https://www.lvhn.org/privacy-policy>

“the protection of health information that may identify you as an individual...[and that information is] treated differently than other forms of personal information that [patients] provide.”²

20. On the same web page, LVHN has a link to its formal “Health Information Privacy Notice,” which acknowledges its obligation to reasonably safeguard sensitive information against security breaches and other types of theft and misuse.


21. As described throughout this Complaint, LVHN did not reasonably protect, secure, or store Plaintiff’s and the Class’s Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information LVHN maintained. Consequently, cybercriminals circumvented Defendant’s security measures, resulting in a significant data breach.

B. The Data Breach

22. On February 6, 2023, LVHN alleges that it detected unauthorized activity on its IT system of a malicious actor who gained unauthorized access to LVHN’s computer network and systems. LVHN launched an investigation and discovered that notorious cyber-hackers, ALPHV, also known as BlackCat, were responsible for the attack. ALPHV has become notorious for launching cyberattacks against academia and healthcare institutions.

² *Id.*

23. ALPHV is also ruthless in its quest for ransom payments. In July 2022, ALPHV announced on Twitter that it was creating a searchable “repository” of data stolen from various companies in order to make it “more usable for the cybercriminal community.” The group made clear its purpose was to “make it easier to find documents, confidential information about companies and employees” and by doing so will “make companies reconsider attitude towards leaks[.]”

 2022-07-05

SupportALPHV Hi

We have something new and very cool today.

Dear Adverts!

We bring to your attention a new view on corporate leaks, and with it a tool for breach-surfing - ALPHV Collections. Resources with leaks posted in our secure repository are now indexed and searchable by wildcard(*). Search by filename as well as by content, e.g. you can find text in PDF, DOCX, even JPG,PNG, etc!

What is the purpose of this?

We want to make the published data more usable for the cybercriminal community. We want to make it easier to find documents, confidential information about companies or employees during OSINT, passwords for dictionaries, etc. By doing so, we will make companies reconsider their attitude towards leaks, separating leaks “on paper” from real leaks.

In the very near future, ALL the published companies will be placed on the same resource with a clear net pass-through.

Translated with www.DeepL.com/Translator (free version)

24. On February 20, 2023, LVHN publicly disclosed that it was the victim of an ALPHV’s cyberattack. LVHN did not disclose whose data was stolen, from what time period, or how much Sensitive Information may have been compromised. LVHN stated only that, it believed “the attack was focused on the Delta Medix IT system” and that LVHN would “provide notices as required to those whose information was involved.” Those notices are yet to be provided.

25. Plaintiff saw the media coverage of the breach and on February 28, 2023, she emailed her physicians asking whether or not her personal Sensitive Information was lost. At that point, Plaintiff had no idea that LVHN stored nude images of her on its computer network.

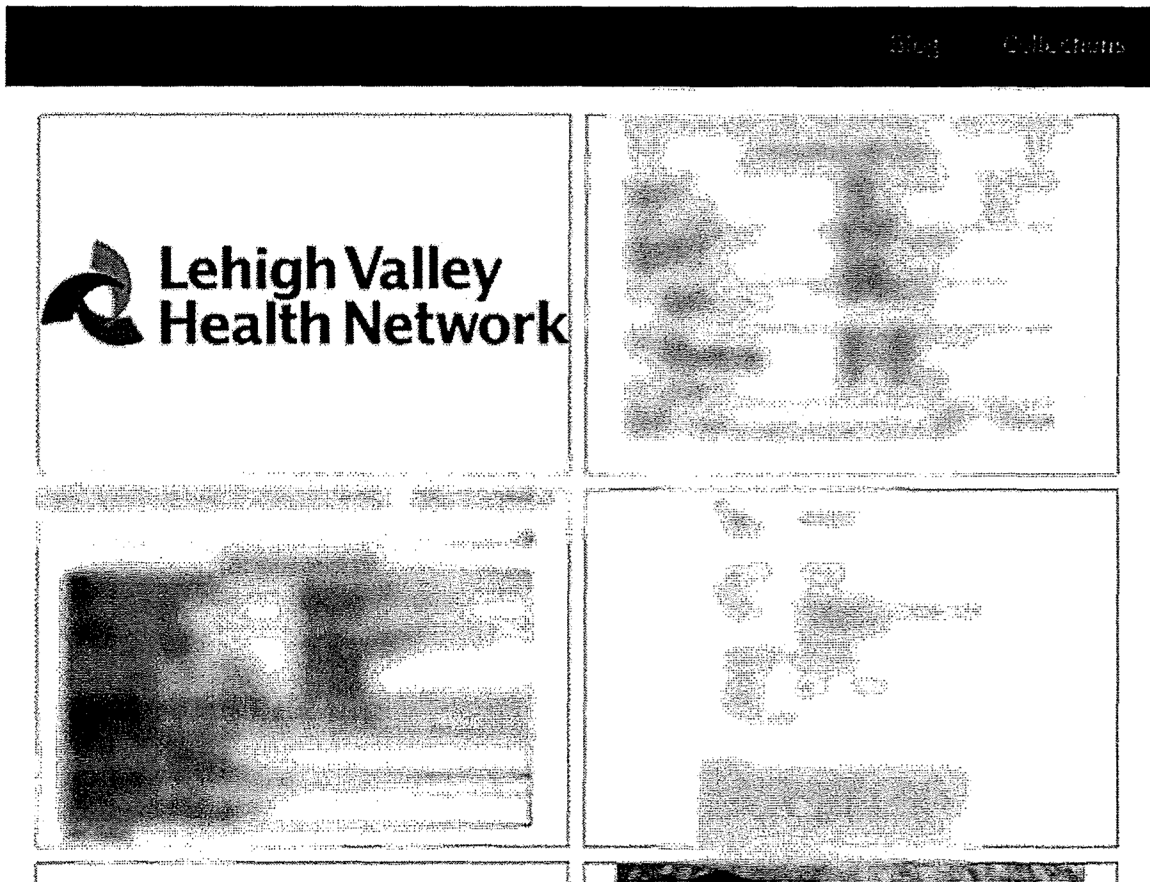
26. On March 4, 2023, the hackers posted a public message to LVHN warning that if it did not meet their ransom demands they would publicly post stolen data, including nude photos of cancer patients receiving treatment. LVHN refused the hackers' demands.

Lehigh Valley Health Network

3/4/2023, 11:02:46 PM

We have been in your network for a long time and have had time to study your business. In addition, we have stolen your confidential data and are ready to publish it. We have the data of your client base of patients, namely their passports, personal data, questionnaires, nude photos and the like. Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business. Your time is running out. We are ready to unleash our full power on you!

27. After LVHN refused the ransom demand, ALPHV posted certain stolen data from LVHN on the dark web. As they warned they would do, ALPHV posted nude photographs of Plaintiff, as well as other yet to be identified cancer patients. An image from ALPHV website showing some select data from the breach posted online.



28. On March 6, 2023, LVHN's Vice President of Compliance, Mary Ann LaRock, contacted Plaintiff telephonically and advised that nude images of her taken during radiation treatment were posted on the dark web by the hackers. Ms. LaRock offered Plaintiff an apology, and with a chuckle, two-years of credit monitoring. Ms. LaRock informed Plaintiff that her Sensitive Information was stolen in the Data Breach, including likely her address, email address, date of birth, Social Security number, health insurance provider, medical diagnosis/medical treatment information, medications, and lab results, in addition to the now public photographs of her receiving breast cancer treatment.

29. In complete disbelief of what she was told, Plaintiff contacted the Dunmore Police and spoke with Officer David Aronica. Officer Aronica informed her that he was aware of a prior

data breach at Delta Medix (the predecessor to LVHN) where Social Security numbers were lost. Officer Aronica agreed to complete a police report on Plaintiff's behalf.

30. Yet, LVHN still refused to give into the hackers, and as a consequence on March 10, ALPHV uploaded an additional 132 gigabyte file onto the dark web, which the hackers described as containing additional patient data and photos. ALPHV promises to leak more patient data and images every week until the ransom is paid.

31. Given that LVHN is and was storing the Sensitive Information of Plaintiff and the Class, including nude photographs of Plaintiff receiving sensitive cancer treatment, LVHN knew or should have known of the serious risk and harm that would occur from a data breach.

32. LVHN was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That obligation stems from the foreseeable risk of a Data Breach given that LVHN collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different healthcare institutions and providers put LVHN on notice that the higher personal data it stored might be targeted by cybercriminals.

33. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry and the prevalence of health care data breaches, LVHN inexplicably failed to adopt sufficient data security processes.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm

34. The personal, health, and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

35. LVHN's failure to reasonably safeguard Plaintiff's and the Class's Sensitive Information has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft.³

36. According to experts, one out of four data breach notification recipients become a victim of identity fraud.⁴ This is because stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

37. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

38. The FBI's Internet Crime Report for 2021 estimated there was more than \$6.9 billion in losses due to phishing scams, non-payment/non-delivery scams, and personal data breach, closely followed by identity theft and extortion.

39. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former

³ The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. 17 C.F.R. § 248.201 (2013).

⁴ *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (last visited Jan. 17, 2022), <https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/>

Commissioner Pamela Jones Harbour underscored this point by reiterating that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”⁵

40. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business.

According to the FTC, reasonable data security protocols require:

- (1) encrypting information stored on computer networks;
- (2) retaining payment card information only as long as necessary;
- (3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;
- (4) limiting administrative access to business systems;
- (5) using industry unapproved activity;
- (6) monitoring activity on networks to uncover unapproved activity;
- (7) verifying that privacy and security features function properly;
- (8) testing for common vulnerabilities; and
- (9) updating and patching third-party software.⁶

41. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts,

⁵ Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf>.

⁶ *Start With Security, A Guide for Business*, FTC (last visited Jan. 18, 2022) <https://www.ftc.gov/system/files/documents/plain-language/pdf0205>.

configuring access controls, disabling remote desktop protocol, and updating and patching computers.

42. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.⁷ Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like LVHN failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

D. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

43. Data breaches have become alarmingly commonplace in the U.S. In 2021, data breaches increased by nearly 70% over the previous year, which is over 20% higher than the previous all-time high.⁸

44. The healthcare sector was the easiest “mark” among all major sectors last year, meaning it had the highest number of data compromises and categorically had some of the most widespread exposure per data breach.⁹ According to the 2021 Healthcare Information and Management Systems Society Cybersecurity Survey, 67% of participating hospitals reported having a significant security incident within the last twelve months, with a majority of those being caused by “bad actors.”¹⁰

⁷ See Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

⁸ 2021 Annual Data Breach Year-End Review, ITRC, (Jan. 2022), <https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/>

⁹ *Id.*

¹⁰ 2021 HIMSS Cybersecurity Survey, Healthcare Information and Management Systems Society, Inc., accessible at: <https://www.himss.org/resources/himss-healthcare-cybersecurity-survey> (last accessed Mar. 16, 2022).

45. Healthcare providers and vendors that maintain health care provider data have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.¹¹

46. A 2010 report focusing on healthcare data breaches found the “average total cost to resolve an identity theft related incident ... came to about \$20,000.”¹² According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.¹³ Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.¹⁴

47. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.¹⁵

¹¹ Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), <https://www.idigitalhealth.com/news/how-to-safeguard-hospitaldata-from-email-spoofing-attacks>.

¹² See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), (last visited Jan. 11, 2021), <https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/>

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), <https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records,close%20to%2021%20million%20records> (last visited Jan.19, 2022).

48. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.¹⁶ For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.¹⁷

49. As a healthcare provider with several thousands of current and former patients, if not more, LVHN knew or should have known the importance of protecting the Sensitive Information entrusted to it.

50. LVHN also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiff and the Class because of the Data Breach. Despite this, LVHN failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. Plaintiff's and the Class's PHI and PII are Valuable.

51. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or their life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.¹⁸

¹⁶ Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/>.

¹⁷ *Five worthy reads: The never-ending love story between cyberattacks and healthcare*, ManageEngine, <https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.>

¹⁸ *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/> (last visited Jan. 18, 2022).

52. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.¹⁹ For that reason, cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as \$300 per number.²⁰ Those numbers are often then used for fraudulent tax returns.²¹

53. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between \$11.33 and \$16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between \$30.49 and \$44.62."²² This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

54. LVHN's Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PHI.

55. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit

¹⁹ Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Jan. 18, 2022).

²⁰ *Id.*

²¹ *Id.*

²² 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), <https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (last visited Jan. 19, 2022).

to apply for more credit in your name.”²³ If the identity thief applies for credit and does not pay the bill, it will damage victims’ credit and cause a series of other related problems.

56. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

57. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation (“FBI”) has found instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.²⁴

58. Other reports found that PHI is ten times more valuable on the black market than credit card information.²⁵ This is because one’s personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for \$1-2 on the black market, but PHI can sell for as much as \$363 according to the Infosec Institute.²⁶

59. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

²³ Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

²⁴ *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), <https://publicintelligence.net/fbi-healthcare-cyber-intrusions/> (last visited Jan. 18, 2022).

²⁵ Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Jan. 18, 2022).

²⁶ *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Jan. 18, 2022).

60. Because the Sensitive Information exposed in LVHN's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their Sensitive Information.

F. LVHN's Conduct Violates HIPAA

61. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.²⁷

62. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."²⁸ The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.²⁹

63. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8)

²⁷ U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>.

²⁸ U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/security/index.html>.

²⁹ *Id.*

Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.³⁰

64. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data LVHN failed to protect. The Data Breach resulted from LVHN's failure to comply with several of these standards:

- a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that LVHN creates, receives, maintains, and transmits;
- b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;
- c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;
- d. Violation of 45 C.F.R. § 164.308(a)(6)(ii): Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;
- e. Violation of 45 C.F.R. § 164.306(a)(2): Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information;
- f. Violation of 45 C.F.R. § 164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;
- g. Violation of 45 C.F.R. § 164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by their workforce;
- h. Violation of 45 C.F.R. § 164.502, et seq: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

³⁰ *Id.*

- i. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

65. Despite LVHN's failure to reasonably protect Plaintiff's and the Class's Sensitive Information, they have not offered any compensation or adequate remedy considering the significant and long-term risks Plaintiff and the Class face.

PLAINTIFF'S EXPERIENCE

66. Plaintiff is a resident of Dunmore and citizen of Pennsylvania. She is a current patient of LVHN.

67. As a condition of receiving healthcare related services, LVHN required Plaintiff to provide her PII and PHI. Accordingly, Plaintiff provided LVHN with her PII and PHI in order to purchase and receive healthcare services, including her address, email address, date of birth, Social Security number, health insurance provider, medical diagnosis/medical treatment information, medications, and lab results. Plaintiff believed her PII and PHI provided to LVHN for healthcare services would be protected by LVHN.

68. Unbeknownst to her, LVHN also took and stored nude photographs of Plaintiff receiving radiation treatment for breast cancer. Plaintiff was not advised that these photographs would be taken and stored on LVHN's network.

69. On February 28, 2023, Plaintiff became aware of the data breach from news reporting. She proactively emailed her physicians asking whether they knew if her information was stolen. The physicians did not respond. On March 6, 2023, however, Plaintiff received a telephone call from LVHN's Vice President of Compliance, who informed her that she was a victim of the Data Breach and that the previously unknown nude photos of her chest and face had

been posted on the dark web. LVHN offered Plaintiff an apology, and two years of credit monitoring.

70. Plaintiff telephoned the Dunmore Police and spoke with Officer Aronica who agreed to complete a police report.

71. Plaintiff also called credit bureaus to warn that her Sensitive Information was part of a data breach. She also telephoned her bank to request that it put fraud alerts on her accounts. Fearing the bank would not follow through, she also drove to her local bank branch headquarters and, in fact, discovered the bank had not placed a fraud alert on her accounts. She waited at the bank until she received confirmation that such an alert was in place. In total, Plaintiff has already spent hours protecting herself from the present and continuing risk of identity theft posed by the Data Breach.

72. Plaintiff is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts. Finally, to her knowledge, Plaintiff has never previously had her identity stolen.

73. Plaintiff suffered actual injury from having her sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) entrusting PII and PHI to LVHN that she would not have had it disclosed it lacked data security practices adequate to safeguard its patients; (b) public disclosure of nude photographs which resulted in embarrassment and humiliation. Those photographs will live eternally on the internet; (c) loss of her privacy; (d) continuous imminent and impending injury arising from the increased risk of financial, medical,

and identity fraud and theft; and (e) time and expense of her mitigation efforts as a result of the data breach.

74. In addition, knowing that hackers accessed and/or stole her Sensitive Information and that this will likely be used in the future for identity theft, fraud, and related purposes has caused Plaintiff experiences feelings of rage, anger, anxiety, sleep disruption, stress, and fear. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

CLASS ALLEGATIONS

75. Pursuant to Pennsylvania Rules of Civil Procedure 1702, 1708, and 1709, Plaintiff bring this action on behalf of herself and on behalf of all members of the proposed Class defined as:

All persons who are identified to be subject of the Data Breach incident at LVHN discovered on or around February 5, 2023.

76. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) LVHN, LVHN's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which LVHN or its parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and LVHN's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

77. Plaintiff and members of the Class satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Pennsylvania Rules of Civil Procedure 1702, 1708, and 1709.

78. **Numerosity, Pennsylvania Rule of Civil Procedure 1702(1):** The exact number of members of the Class are unknown but, upon information and belief, they are estimated to number in the hundreds if not thousands, and individual joinder in this case is impracticable. Members of the Class can be easily identified through LVHN's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

79. **Typicality, Pennsylvania Rule of Civil Procedure 1702(3):** Plaintiff's claims are typical of the claims of other members of the Class in that Plaintiff, and the members of the Class sustained damages arising out of LVHN's Data Breach, wrongful conduct and misrepresentations, concealment, and unlawful practices, and Plaintiff and members of the Class sustained similar injuries and damages, as a result of LVHN's uniform illegal conduct.

80. **Adequacy, Pennsylvania Rule of Civil Procedure 1702(4) and 1709:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and LVHN has no defenses unique to Plaintiff.

81. **Commonality and Predominance, Pennsylvania Rule of Civil Procedure 1702(2) and 1708(a)(1):** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- a. Whether LVHN violated the laws asserted herein;

- b. Whether LVHN had a duty to use reasonable care to safeguard Plaintiff's and members of the Class's PII and PHI;
- c. Whether LVHN breached the duty to use reasonable care to safeguard members of the Class's PII and PHI;
- d. Whether LVHN knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive PII and PHI;
- e. Whether LVHN failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and members of the Class's PII and PHI from unauthorized release and disclosure;
- f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within LVHN's computer systems to safeguard and protect Plaintiff's and members of the Class's PII and PHI from unauthorized release and disclosure;
- g. Whether Plaintiff and members of the Class were injured as a proximate cause or result of the Data Breach;
- h. What the proper measure of damages is; and
- i. Whether Plaintiff and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

82. **Manageability – Pennsylvania Rule of Civil Procedure 1708(a)(2):** The claims of Plaintiff and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiff and the Class.

83. **Risk of Inconsistent, Varying or Prejudicial Adjudications – Pennsylvania Rule of Civil Procedure 1708(a)(3):** If the claims of Plaintiff and the Class were tried separately, LVHN may be confronted with incompatible standards of conduct and divergent court decisions. Furthermore, if the claims of Plaintiffs and the members of the Class were tried individually,

adjudications with respect to individual Class Members and the propriety of their claims could be dispositive on the interests of other members of the Class not party to those individual adjudications and substantially, if not fully, impair or impede their ability to protect their interests.

84. Litigation Already Commenced – Pennsylvania Rule of Civil Procedure

1708(a)(4): To Plaintiffs' knowledge, there are no other cases that have been brought against LVHN, or that are currently pending against LVHN, where a Pennsylvania consumer seeks to represent a class of Pennsylvania residents based on the conduct alleged in this Class Action Complaint.

85. The Appropriateness of the Forum – Pennsylvania Rule of Civil Procedure

1708(a)(5): This is the most appropriate forum to concentrate the litigation because Plaintiff resides in this county and LVHN conducts business in this county

86. The Class Members' Claims Support Certification – Pennsylvania Rule of

Civil Procedure 1708(a)(6) and (7): Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits. Furthermore, the damages that may be recovered by the Class will not be so small such that class certification is unjustified.

87. The General Applicability of LVHN's Conduct – Pennsylvania Rule of Civil

Procedure 1708(b)(2): LVHN's failure to secure PII and PHI is generally applicable to the Class as a whole, making equitable and declaratory relief appropriate with respect to each Class Member.

CLAIMS FOR RELIEF

COUNT I

Negligence

(On behalf of Plaintiff and the Class)

A. General Negligence

88. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

89. LVHN collected, created, and maintained Plaintiff's and the Class's Sensitive Information for the purpose of providing medical or related services to Plaintiff and the Class.

90. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that LVHN was aware, or should have been aware, could be injured by inadequate data security measures. The nature of LVHN's business requires patients to disclose Sensitive Information to receive adequate care, including, but not limited to, medical histories, dates of birth, addresses, phone numbers, and medical insurance information. Thus, for LVHN to provide its services, it must use, handle, gather, and store the Sensitive Information of Plaintiff and the Class and, additionally, solicit and create records containing Plaintiff's and the Class's Sensitive Information.

91. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. LVHN knew or should have known that, given its repository of a host of Sensitive Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, LVHN had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

92. LVHN owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

93. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the Class's PHI and PII was adequately protected and secured. LVHN further had a duty to implement processes that would detect a breach of its security system in a timely manner.

94. LVHN also should have known that, given the Sensitive Information it held, Plaintiff and the Class would be harmed should it suffer a Data Breach. LVHN knew or should have known that its systems and technologies for processing and securing Plaintiff's and the Class's PHI and PII had security vulnerabilities susceptible to cyber-attacks.

95. Despite that knowledge, LVHN failed to implement reasonable data security measures which allowed cybercriminals to successfully breach LVHN's network and data environments, reside there undetected for a period of time, and access or steal a host of personal and healthcare information from LVHN's patients.

96. LVHN, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

97. LVHN breached its duty to Plaintiff and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiff's and the Class's PHI and PII. LVHN further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's PHI and PII.

98. But for LVHN's wrongful and negligent breach of its duties, their Sensitive Information would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

99. As a result of LVHN's negligence, Plaintiff and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of LVHN's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

100. As a direct and proximate result of LVHN's negligence, Plaintiff and members of the Class suffered and continue to suffer injuries and are entitled to and demand actual, consequential, and nominal damages in an amount to be proven at trial.

B. Negligence *Per Se*, Violation of 15 U.S.C. § 45

101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted, and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of LVHN's duty.

102. LVHN violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PHI and PII and not complying with industry standards. LVHN's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

103. LVHN's violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. Plaintiff and the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

105. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures, caused the same harm suffered by Plaintiff and the proposed Class.

106. As a direct and proximate result of LVHNs' negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries as described herein and are entitled to damages in an amount to be proven at trial.

C. Negligence Per Se, Violation of HIPAA, 45 C.F.R. § 160.102

107. LVHN required Plaintiff and the Class to provide nonpublic Sensitive Information to obtain medical services. During the provision of those services, LVHN created and stored even more PHI.

108. As a healthcare provider, LVHN is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

109. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

110. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as LVHN. HIPAA standards are mandatory.

111. HIPAA requires LVHN to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably

anticipated threats or hazards to the security or integrity” of the Sensitive Information. 45 C.F.R. § 164.306.

112. LVHN violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

113. LVHN violated HIPAA by failing to use reasonable measures to protect the PII and PHI of Plaintiffs and Class. LVHN’s conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

114. LVHN’s violation of HIPAA constitutes negligence *per se*. Plaintiff and the Class are within the group of individuals HIPAA was designed to protect and the harm to these individuals is a result of the Data Breach.

115. As a direct and proximate result of LVHNs’ negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries as described herein and are entitled to damages in an amount to be proven at trial.

COUNT II

Breach of Fiduciary Duty

(On behalf of Plaintiff and the Class)

116. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

117. Plaintiff and the Class incorporate the above allegations as fully set forth herein.

118. LVHN owed a fiduciary duty to Plaintiff and the Class to protect their private and sensitive PHI and PII and keep them apprised of when that information becomes exposed or compromised in an accurate manner.

119. LVHN breached that fiduciary duty by, *inter alia*, failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Class. This failure resulted in the Data Breach that ultimately came to pass.

120. As a direct and proximate cause of LVHN's breaches of its fiduciary duty, Plaintiff and the Class members have suffered and will suffer injury, including but not limited to: (a) the compromise, publication, theft, and /or unauthorized use of their PII and PHI; (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to their PII and PHI, which remains in the possession of LVHN and is subject to further breaches so long as LVHN fails to undertake appropriate measures to protect PII and PHI in its possession; and (e) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and members of the Class.

121. Plaintiff, on behalf of herself and the Class, seeks actual, consequential, and nominal damages and injunctive relief for breach of fiduciary duty.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Proposed Class)

122. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

123. LVHN offered to provide medical goods and services to Plaintiff and the Class in exchange for payment.

124. LVHN also required Plaintiff and the members of the Class to provide LVHN with their PHI in order to receive goods and services.

125. In turn, and through the Privacy Policy, LVHN agreed it would not disclose the PHI it collects from patients to unauthorized persons. LVHN also promised to maintain safeguards to protect its patients' PHI.

126. Plaintiff and the members of the Class accepted LVHN's offer by providing PHI to LVHN in exchange for receiving LVHN's goods and services and then by paying for and receiving the same.

127. Plaintiff and the members of the Class would not have entrusted their PHI to LVHN in the absence of such agreement with LVHN.

128. LVHN materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information. LVHN further breach the implied contracts with Plaintiff and members of the Class by:

- a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PHI;
- b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;
- c. Failing to ensure the confidentiality and integrity of electronic PHI that LVHN created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

129. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of LVHN's material breaches of its agreement(s).

130. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of the LVHN.

131. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honest in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit – not merely the letter – of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

132. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

133. In these and other ways, LVHN violated its duty of good faith and fair dealing.

134. Plaintiff and members of the Class have sustained damages as a result of LVHN's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and the Proposed Class)

135. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

136. At all times during Plaintiff's and Class Members' interactions with LVHN, LVHN was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' personal data that Plaintiff and Class Members provided to LVHN.

137. As alleged herein and above, LVHN's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' personal data would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

138. Plaintiff and Class Members provided their respective personal data and health information to LVHN with the explicit and implicit understandings that LVHN would protect and not permit the personal data to be disseminated to any unauthorized parties.

139. Plaintiff and Class Members also provided their respective personal data to LVHN with the explicit and implicit understanding that LVHN would take precautions to protect that personal data from unauthorized disclosure, such as following basic principles of information security practices.

140. LVHN voluntarily received in confidence Plaintiff's and Class Members' personal data with the understanding that the personal data would not be disclosed or disseminated to the public or any unauthorized third parties.

141. Due to LVHN's failure to prevent, detect, and/or avoid the data breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' personal data, Plaintiff's and Class Members' personal data was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

142. As a direct and proximate cause of LVHN's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

143. But for LVHN's disclosure of Plaintiff's and Class Members' personal data in violation of the parties' understanding of confidence, their personal data would not have been

compromised, stolen, viewed, accessed, and used by unauthorized third parties. LVHN's Data breach was the direct and legal cause of the theft of Plaintiff's and Class Members' personal data, as well as the resulting damages.

144. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of LVHN's unauthorized disclosure of Plaintiff's and Class Members' personal data. LVHN knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' personal data had numerous security vulnerabilities because LVHN failed to observe industry standard information security practices.

145. As a direct and proximate result of LVHN's breaches of confidence, Plaintiff's and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

146. As a direct and proximate result of LVHN's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Publicity Given to Private Life
(On Behalf of Plaintiff and the Class)

147. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

148. One who gives publicity to matters concerning the private life of another, of a kind highly offensive to a reasonable man, is subject to liability to the other for invasion of his privacy.

149. Plaintiff and the Class provided LVHN with sensitive personal information, including names, Social Security numbers, financial account information, as well as personal health information and photographs of themselves in stages of undress.

150. LVHN failed to employ adequate and reasonable security measures to prevent public disclosure of Plaintiff and the Class's private information.

151. As a result of the disclosure of Plaintiff's and the Class's private information, Plaintiff and the Class have suffered a *de facto* injury, which entitles them to general damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully pray for judgment in their favor as follows:

- a. Certification of the Class pursuant to the provisions of Pennsylvania Rule of Civil Procedure 1702 and an order that notice be provided to all Class Members;
- b. Designation of Plaintiff as representatives of the Class and the undersigned counsel, as Class Counsel;
- c. An award of damages in an amount to be determined at trial or by this Court;
- d. An award of punitive damages for LVHN's reckless, wanton, and willful conduct in allowing nude images of cancer patients to be knowingly posted on the internet;

e. An order for injunctive relief, enjoining LVHN from engaging in the wrongful and unlawful acts described herein;

f. Pre-judgment interest at the maximum amount allowed by law;

g. Post-judgment interest at the maximum rate allowed by law;

h. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury of all issues so triable.

Respectfully submitted,

Dated: March 13, 2023

By: 

Todd J. O'Malley, Esq.

Mary Anne O. Lucas, Esq.

O'MALLEY & LANGAN

201 Franklin Avenue

Scranton, PA 18503

Tel: (570) 344-2667

Fax: (570) 344-6199

tomalley@omalleylanguan.com

mlucas@omalleylanguan.com

Simon B. Paris, Esq.

Patrick Howard, Esq. (PA ID #88572)

SALTZ, MONGELUZZI, & BENDESKY, P.C.

1650 Market Street, 52nd Floor

Philadelphia, PA 19103

Tel: (215) 496-8282

Fax: (215) 496-0999

phoward@smbb.com

Samuel J. Strauss, Esq.

Raina Borrelli, Esq.*

TURKE & STRAUSS LLP

613 Williamson Street, Suite 201

Madison, Wisconsin 53703

Tel: (608) 237-1775

Fax: (608) 509-4423

sam@turkestrauss.com

raina@turkestrauss.com

*To be admitted *pro hac vice*

Counsel for Plaintiff and the Proposed Class

MAURIB. KELLY
LACKAWANNA COUNTY
2023 MAR 13 P 2:51
CLERK OF JUDICIAL
RECORDS CIVIL DIVISION

VERIFICATION

The averments or denials of fact contained in the foregoing document are true based upon the personal knowledge or information and belief of the signer. If the foregoing contains averments which are inconsistent in fact, the signers have been unable, after reasonable investigation, to ascertain which of the inconsistent averments are true, but signer has knowledge or information sufficient to form a belief that one of them is true. This Verification is made subject to the penalties of 18 Pa.C.S. § 4904, relating to falsification to authorities.


JANE DOE

**IN THE COURT OF COMMON PLEAS
FOR LACKAWANNA COUNTY**

Jane Doe,

Court File No.: 23-CV-1149

*Individually and on behalf of all others
similarly situated,*

Plaintiff,

vs.

Lehigh Valley Health Network, Inc.

Defendant.

**PLAINTIFF DOE'S MOTION AND
INCORPORATED MEMORANDUM
OF LAW IN SUPPORT OF
PRELIMINARY INJUNCTION
WITHOUT HEARING**

INTRODUCTION

Plaintiff Jane Doe ("Plaintiff") and the putative Class Members seek a preliminary injunction without hearing pursuant to Pa. R. Civ. P. 1531 enjoining Defendant Lehigh Valley Health Network, Inc. ("LVHN") to meet the ransom demand of the data hackers known as, ALPHV in order to prevent the release of further nude pictures and private health and personal information of the Plaintiff and the Class Members. The additional release of such private, personal, and sensitive information for public consumption constitutes immediate an irreparable harm that warrants such an injunction. *See Pennsylvania State Educ. Ass'n ex rel. Wilson v. Com., Dept. of Community and Economic Development, Office of Open Records*, 981 A.2d 383 (Pa. Cmwlth. 2009). At bottom, our privacy is sacrosanct and is a pillar of our American Civil Liberties. Once an individual's right to privacy is breached, it cannot be undone. The Court should act to stop others from befalling the same fate as Plaintiff Doe.

In addition, Plaintiff seeks an order requiring LVHN to notify all those who have are believed to have been a victim of the data breach so they can immediately take steps to protect themselves. The Pennsylvania Legislature passed the Breach of Personal Information Notification Act (Data Breach Act), 73 P.S. §§ 2301-2329. Under the Data Breach Act, the

Legislature has imposed a duty on entities, like LVHN, to provide notice of a data breach, 73 P.S. § 2303. LVHN should be ordered to comply with its legal requirements and provide notice to all those reasonably believed to be impacted.

BACKGROUND

Plaintiff and the putative Class Members are individuals who were subject to the Data Breach incident at LVHN which occurred on or around January 8, 2023, which LVHN discovered on or around February 6, 2023. In the underlying class action complaint, Plaintiff alleges that LVHN failed to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used in its ordinary course of business. Class Action Complaint, Dkt. No. 1, at ¶ 9.

LVHN alleges that it detected unauthorized activity on its IT system and, upon subsequent investigation, discovered that notorious cyber-hackers ALPHV, also known as BlackCat, were responsible for the attack. *Id.*, at ¶ 22. LVHN publicly disclosed that it was the victim of ALPHV's cyberattack on February 20, 2023, and stated that it would "provide notices as required to those whose information was involved." *Id.*, at ¶ 24.

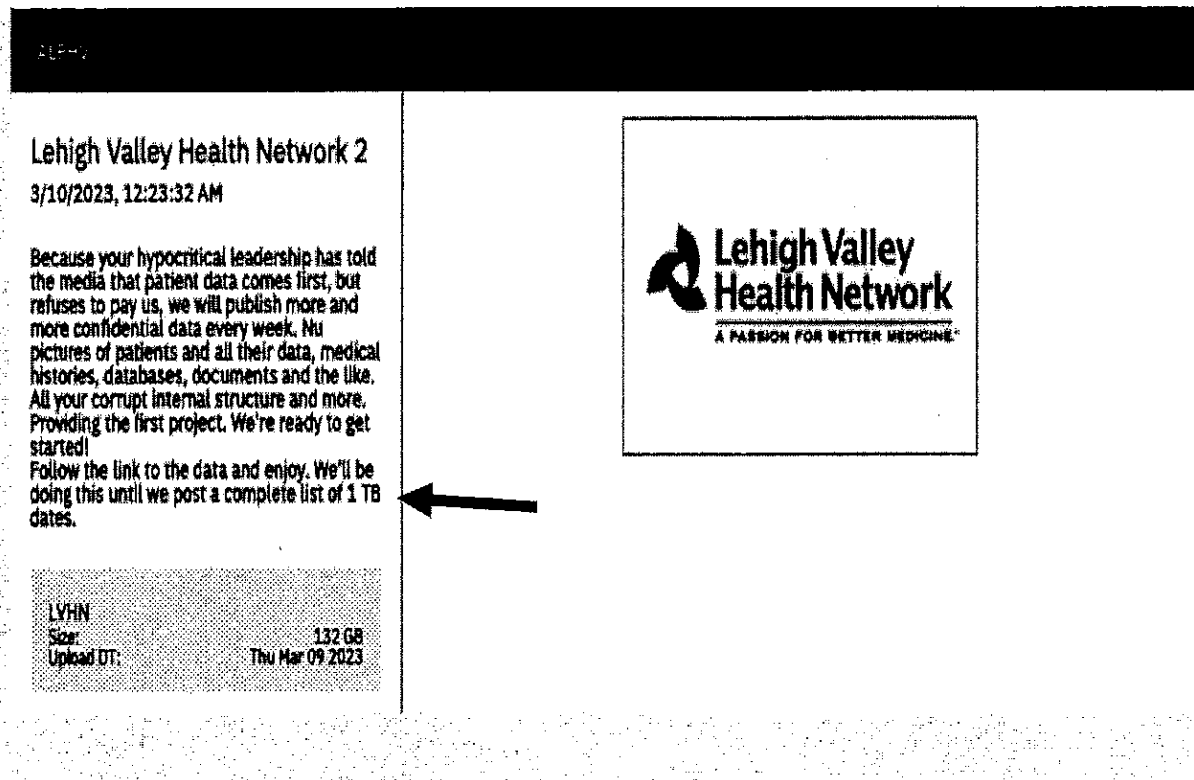
ALPHV posted a public message to LVHN on March 4, 2023, warning that if LVHN did not meet its ransom demands, ALPHV would publicly post stolen data. This message specifically referenced nude photos, which were taken of cancer patients while they were receiving treatment at LVHN. *Id.*, at ¶ 26. When LVHN refused the ransom demand, ALPHV posted nude photographs of Plaintiff and other cancer patients onto the dark web. *Id.*, at ¶ 27.

LVHN's Vice President of Compliance, Mary Ann LaRock, contacted Plaintiff telephonically on March 6, 2023, and advised that nude images of Plaintiff taken during radiation treatment were posted on the dark web by ALPHV and that other protected health information

(“PHI”) and personally identifiable information (“PII”) had also been stolen in the data breach.

Id., at ¶ 28. Plaintiff did not know that LVHN stored nude images of her on its computer network until this time. CAC, at ¶ 25.

On March 10, 2023, after LVHN continued to refuse to meet ALPHV’s ransom demands, ALPHV uploaded an additional 132 gigabyte file onto the dark web. This file contained additional patient data and nude photos. ALPHV claims to have 1 terabyte of data from LVHN’s network and promises to continue leaking patient data and photographs until LVHN pays the ransom. *Id.*, at ¶ 30. An image from the ALPHV website showing the post of 132 GB of data on the dark web and warning about additional postings of the 1 TB of data.



Plaintiff filed this class action on behalf of herself and all persons who are identified to be subject of the Data Breach incident at LVHN that was discovered on or around February 5, 2023. Dkt. No. 1, at ¶ 75. Now, Plaintiff, on behalf of herself and all other similarly situated, brings the

instant Motion for a preliminary injunction enjoining Defendant from continuing to neglect its duty to Plaintiff and Class Members to protect their PHI and PII and require Defendant to meet the ransom demands of ALPHV in order to prevent further release of this information, and specifically the nude photographs obtained through the Data Breach. Plaintiff also requests the Court order LVHN to immediately notify all victims of the breach as required by the Data Breach Act.

LEGAL STANDARD

A party seeking a preliminary injunction must satisfy five factors. The movant must show (1) that the injunction is necessary to prevent immediate and irreparable harm that cannot be adequately compensated by damages; (2) that greater injury would result from refusing an injunction than from granting it and that the injunction will not substantially harm other interested parties; (3) that the preliminary injunction will restore the parties to their status quo as it existed prior to the alleged wrongful conduct; (4) that the moving party it is likely to prevail on the merits; (5) that the injunction it seeks is reasonably suited to abate the offending activity and (6) that the preliminary injunction will not adversely affect the public interest. *Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mount, Inc.*, 573 Pa. 637, 646–47, 828 A.2d 995, 1001 (2003).

Under Pa. R. Civ. P. 1531, “[a] court shall issue a preliminary or special injunction only after written notice and hearing unless it appears to the satisfaction of the court that immediate and irreparable injury will be sustained before notice can be given or a hearing held, in which case the court may issue a preliminary or special injunction without a hearing or without notice.” Pa. R. Civ. P. 1531(a) (2003). In determining whether a preliminary injunction should be granted and whether notice or a hearing should be required, the court may act on the basis of the pleadings. *Id.* Pennsylvania courts have held that a preliminary injunction without hearing is the

“functional equivalent” to a temporary restraining order. *Greater Nanticoke Area Educ. Ass'n v. Greater Nanticoke Area Sch. Dist.*, 938 A.2d 1177, 1181–82 (Pa. Commw. Ct. 2007) (citing *Bloomington's by Mail Ltd. v. Dep't of Revenue*, 513 Pa. 149, 153, 518 A.2d 1203, 1205 n. 3 (Pa. 1986); *E. Stroudsburg Univ. v. Hubbard*, 591 A.2d 1181 (Pa. Commw. Ct. 1991)).

ARGUMENT

I. PLAINTIFF AND CLASS MEMBERS WILL SUFFER IMMEDIATE AND IRREPARABLE HARM IF A PRELIMINARY INJUNCTION IS NOT GRANTED

The first factor that courts consider in determining whether a preliminary injunction should be granted is whether the relief being sought is necessary to prevent immediate and irreparable harm that cannot be adequately compensated by money damages. *Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mountain*, 573 Pa. at 646–47. In this case, Plaintiff and Class Members are suffering and will continue to suffer immediate irreparable harm if the Defendant is not ordered to pay the ransom demand to prevent further release of information. ALPHV has promised to release more information, and specifically more nude photos, on a weekly basis until LVHN meets the ransom demands. As demonstrated from the multiple releases of information, the potential for increased harm is ongoing.

To show that the immediate and irreparable harm cannot be compensated by money damages, Plaintiff and Class Members must present “concrete evidence demonstrating actual proof of irreparable harm” which cannot be solely based on “speculation and hypothesis” and must be “irreversible”. *Greenmore, Inc. v. Burchick Const. Co., Inc.*, 908 A.2d 310, 314 (Pa. Super. Ct. 2006) (internal quotations and citations omitted). In *Sovereign Bank v. Harper*, the Superior Court of Pennsylvania acknowledged the Pennsylvania Supreme Court’s approval of an injunction that the harm would be irreparable “because the extent of the injury was inherently

unascertainable, and hence incapable of being fully compensated by money damage.” 674 A.2d 1085, 1093 (Pa. Super. Ct. 1996).

The release of nude photographs, along with PHI and PII, cannot be adequately compensated by money damages. Once data is release to the dark web, it cannot be removed.¹ Data breach victims must resort to other costly methods of trying to protect themselves, but, as the information will still be accessible to dark web users, they live under the life-long threat of malicious use of that information. It is truly an irreversible harm with unbounded consequences.

But this is not simply a case in which social security numbers or dates of birth are being disclosed, which in and of itself, causes irreparable harm. This is a case in which thousands of nude photographs of patients who are undergoing cancer treatment are being released onto the dark web. Often, the patients were not even aware the photos were being taken. So, in addition to the time-consuming and costly efforts to mitigate the actual and potential impact on their financial well-being, the Plaintiff and Class Members will suffer embarrassment and humiliation by having these nude images of themselves taken at a time when they were most vulnerable posted on the internet. Like the PHI and PII released to the dark web, these photographs cannot be removed. And now, they must continue to fear that additional photos and information will also be posted because the Defendant refuses to pay the ransom to protect their patients’ private information. Whether or not the continued disclosures of these deeply personal photographs as well as their PHI and PII are posted on the web can be prevented by issuing the requested injunction.

Plaintiff also alleges that by failing to use reasonable measure to protect Plaintiff’s and Class Members’ PII and PHI from further disclosure by paying the ransom, Defendant has

¹ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

violated section 5 of the FTC Act, 15 U.S.C. § 45, and violated HIPAA, 45 C.F.R. § 160.102, by failing to adhere to and meet the requirement of 45 CFR §§ 164.308, 164.310, 164.312, 164.314, 164.316. Dkt. No. 1, at ¶¶ 101–115. “The violation of a statute constitutes immediate and irreparable harm and issuing a preliminary injunction to avoid such a violation is justified.” *Central Dauphin Educ. Ass’n v. Central Dauphin School Dist.*, 792 A.2d 691, 698 (Pa. Commw. Ct. 2001) (quoting *Public Utility Commission v. Israel*, 356 Pa. 400, 406, 52 A.2d 317, 321 (Pa. 1947)).

II. GREATER INJURY WOULD RESULT IF THE COURT WERE TO NOT GRANT THE INJUNCTION THAN IF THE INJUNCTION WERE GRANTED

The Court should also weigh whether any injury that Defendant may suffer as a result of the injunction would be greatly outweighed by the injury to Plaintiff and Class Members if the injunction was not granted. *See Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mountain*, 573 Pa. at 647. This injunction would require LVHN to pay ALPHV the demanded ransom. While this may cause some financial injury to Defendants (which may be recoverable through insurance in any event), this harm is overshadowed by the injuries to Plaintiffs and Class Members that would result from further releases of PII, PHI, and nude photographs.

Courts have repeatedly found that the injuries resulting from the nonconsensual dissemination of nude images to be substantial. In *State v. VanBuren*, the Supreme Court of Vermont found that the state had a compelling interest in criminalizing nonconsensual pornography, in part due to the degree of harm to victims. 214 A.3d 791, 810–11 (Vt. 2019) (discussing potential harm to employment, potential harassment, extortion, unwelcome sexual attention and threats of violence, and risk of extreme emotional distress and suicidal ideation). The Supreme Court of Indiana heavily cited the *VanBuren* decision in finding that a similar statute in Indiana was also not a violation of the First Amendment. *State v. Katz*, 179 N.E.3d

431, 456–58 (Ind. 2022). In its examination of a similar Minnesota statute, the Supreme Court of Minnesota wrote that “[t]hose who are unwillingly exposed to their friends, family, bosses, co-workers, teachers, fellow students, or random strangers on the internet are often deeply and permanently scarred by the experience. Victims suffer from post-traumatic stress disorder, anxiety, depression, despair, loneliness, alcoholism, drug abuse, and significant losses in self-esteem, confidence, and trust.” *State v. Casillas*, 952 N.W.2d 629 (Minn. 2020).

Any injury to LVHN is quantifiable—the amount paid to satisfy the ransom. The injuries to Plaintiff and Class Members have the potential to be personally and economically devastating.

III. GRANTING THE INJUNCTION WOULD RESTORE THE STATUS QUO

The Court should also weigh whether the injunction will restore the parties to their status quo as it existed before the alleged wrongful conduct. *Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mountain*, 573 Pa. at 647. “The relevant standard requires that an injunction must address the status quo as it existed between the parties before the event that gave rise to the lawsuit, not to the situation as it existed after the alleged wrongful act but before entry of the injunction.” *Abrogi v. Reber*, 932 A.D. 969, 979 (Pa. Super. Ct. 2007) (citing *Anchel v. Shea*, 762 A.2d 346, 351 (Pa. Super. Ct. 2000)).

If the Court grants the injunction, Plaintiff and the other putative Class Members will be restored to (as best as able) to the pre-conduct status in that they will no longer have to worry about what additional private information may be put on the dark web. And, although Defendant will be required to pay the ransom in order to protect Plaintiff’s and Class Members’ PHI, PII, and other sensitive information it stored on its network, it also would be restored to its pre-conduct status in that it would once again be taking affirmative steps to prevent further dissemination of Plaintiff and Class Members’ PHI and PII, as it is required by law to do.

IV. PLAINTIFF AND CLASS MEMBERS HAVE A CLEAR RIGHT TO RELIEF AND ARE LIKELY TO PREVAIL ON THE MERITS OF THEIR CLAIMS

The Court must also look at whether the Plaintiff and Class are likely to prevail on the merits of their claims. *Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mountain*, 573 Pa. at 647. “The party seeking an injunction must show that the activity it seeks to restrain is actionable, that its right to relief is clear, and that the wrong is manifest, or, in other words, must show that it is likely to prevail on the merits.” *Id.* When establishing a clear right to relief, “the party seeking an injunction need not prove the merits of the underlying claim, but need only demonstrate that substantial legal questions must be resolved to determine the rights of the parties.” *SEIU Healthcare Pennsylvania v. Com.*, 628 Pa. 573, 590–91, 104 A.3d 495, 506 (2014).

Plaintiff and Class Members have a strong likelihood of success on the merits. Plaintiff has brought claims under Negligence, both General Negligence and Negligence Per Se, in violation of 15 U.S.C. §45 and 45 C.F.R. §160.102. CAC, at ¶¶ 88–115. Plaintiff has also brought a claim for Breach of Fiduciary Duty (*see* CAC, at ¶¶ 116–121); Breach of an Implied Contract (*see* CAC, at ¶¶ 122–134); Breach of Confidence (*see* CAC, at ¶¶ 125–146); and Publicity Given to Private Life (*see* CAC, at ¶¶ 147–151).

In order to prove General Negligence, Plaintiff must show “(1) a duty or obligation recognized by law; (2) a breach of that duty; (3) a causal connection between the conduct and the resulting injury; and (4) actual damages.” *Grossman v. Barke*, 868 A.2d 561, 566 (Pa. Super. Ct. 2005). Plaintiff has alleged that LVHN owed a duty of care to Plaintiff and Class Members to protect their sensitive PII and PHI and that LVHN breached its duty by failing to implement reasonable data security measures. Dkt. No. 1, at ¶¶ 92–97. Plaintiff has alleged that if not for LVHN’s breach of duty, her and Class Members’ PHI and PII would not have been accessed by unauthorized persons. *Id.*, at ¶ 98. Finally, Plaintiff has alleged that she and Class Members have

suffered actual damages as a result, including, but not limited to ongoing and immediate threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; and credit, debit, and financial monitoring. *Id.*, at ¶ 99.

In order to prove Negligence Per Se in violation of 15 U.S.C. § 45 and 45 C.F.R. § 160.102, Plaintiff must show “(1) The purpose of the statute must be, at least in part, to protect the interest of a group of individuals, as opposed to the public generally; (2) The statute or regulation must clearly apply to the conduct of the defendant; (3) The defendant must violate the statute or regulation; (4) The violation of the statute or regulation must be the proximate cause of the plaintiff's injuries.” *Ramalingam v. Keller Williams Realty Group, Inc.*, 121 A.3d 1034, 1042–43 (Pa. Super. Ct. 2015). For the Negligence Per Se claim relating to 15 U.S.C. § 45, Section 5 of the FTC Act, Plaintiff has alleged that she and Class Members are within the class of persons Section 5 of the FTC Act was intended to protect. Dkt. No. 1, at ¶ 104. She has also alleged that Section 5 of the FTC Act, and its interpretation and enforcement by the FTC, applies to the conduct of LVHN regarding Plaintiff's and Class Members' PHI and PII. *Id.*, at ¶ 101. Plaintiff further alleges that by failing to protect her and Class Members' PHI and PII, LVHN has violated Section 5 of the FTC Act and that those violations are the direct and proximate cause of the harm suffered by Plaintiff and Class Members. *Id.*, at ¶¶ 102, 106.

Regarding the Negligence Per Se claim relating to HIPAA, 45 C.F.R. § 160.102, Plaintiff has alleged that she and Class Members are within the class of persons that HIPAA was designed to protect. *Id.*, at ¶ 114. Plaintiff has also alleged the LVHN was covered by HIPAA as a healthcare provider and was therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164. *Id.*, at ¶¶ 108–111. Plaintiff alleged that LVHN violated HIPAA by failing to use reasonable measures to protect Plaintiff and Class Members' PHI and PII. *Id.*, at

¶¶ 112–113. Finally, Plaintiff has alleged that LVHN’s failure to protect her and Class Members’ PHI and PII as required under HIPAA directly and proximately cause harm to her and Class Members. *Id.*, at ¶ 115.

In order to prove Breach of Fiduciary Duty, Plaintiff must show (1) the existence of a fiduciary relationship between her and LVHN, (2) that LVHN negligently or intentionally failed to act in good faith and solely for her benefit, and (3) that Plaintiff suffered an injury caused by LVHN’s breach of fiduciary duty. *Snyder v. Crusader Servicing Corporation*, 231 A.3d 20 (Pa. Super. Ct. 2020). Plaintiff has alleged that a fiduciary relationship existed between her and LVHN where LVHN owed Plaintiff a fiduciary duty. Dkt. No. 1, at ¶ 118. Plaintiff has further alleged that LVHN negligently failed to act in good faith and failed to protect Plaintiff’s and Class Members’ sensitive PHI and PII. *Id.*, at ¶ 119. Ultimately, Plaintiff alleged, this breach caused Plaintiff and Class Members injury. *Id.*, at ¶ 120.

In order to prove Breach of Implied Contract, Plaintiff must show “[(1)] existence of a contract (including its essential terms), [(2)] a breach of duty imposed by the contract and [(3)] resultant damages.” *Young v. Wetzel*, 260 A.3d 281, 290 (Pa. Commw. Ct. 2021). For a contract to exist, there must be (1) an offer, (2) acceptance of the offer, and (3) consideration. *Hatbob v. Brown*, 575 A.2d 607, 613 (Pa. Super. Ct. 1990). Plaintiff has alleged the existence of a contract where LVHN offered to provide medical goods and services and Plaintiff and Class Members accepted that offer in exchange for providing PHI and PII and paying for the medical good and services. Dkt. No. 1, at ¶¶ 123–126. Plaintiff alleges that LVHN breached that contract by failing to protect her and Class Members’ PHI and PII and failing to comply with industry standard and legal obligations incorporated into the agreement through the Privacy Policy. *Id.*, at ¶ 128.

Finally, Plaintiff has alleged that she and Class Members have suffered damages as a result of LVHN's breach of contract. *Id.*, at ¶ 134.

In order to prove Breach of Confidence, Plaintiff must show “(1) the plaintiff conveyed ‘confidential and novel information’ to the defendant; (2) the defendant had knowledge that the information was being disclosed in confidence; (3) there was an understanding between the defendant and the plaintiff that the confidence be maintained; and (4) there was a disclosure or use in violation of the understanding.” *Burns v. Erving*, 810 F. Supp. 2d 1167, 1172 (D. Nev. 2011). Plaintiff has alleged that she and Class Members conveyed intimate PHI and PII to LVHN. Dkt. No. 1, at ¶¶ 138–139. Plaintiff has further alleged that when she and Class Members conveyed this information to LVHN, LVHN knew that this information was being disclosed in confidence, and there was mutual explicit and implicit understanding that this information was to be kept confidential. *Id.*, at ¶¶ 136–140. Plaintiff has also alleged that LVHN failed to protect her and Class Members’ data and a disclosure of that information occurred. *Id.*, at ¶ 141.

In order to prove the final claim of Publicity Given to Private Life, Plaintiff must show “(1) publicity, given to (2) private facts, (3) which would be highly offensive to a reasonable person and (4) is not of legitimate concern to the public.” *Harris by Harris v. Easton Pub. Co.*, 483 A.2d 1377, 1384 (Pa. Super. Ct. 1984). For the purposes of this tort, publicity “requires that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.” *Burger v. Blair Med. Assocs., Inc.*, 964 A.2d 374, 378 (Pa. 2009). Here, Plaintiff alleges that publicity was given to her and Class Members’ private facts by LVHN’s failure to employ adequate and reasonable security measures to prevent disclosure. *Id.*, at ¶ 149–150. The private facts here, including Social Security numbers, financial information, PHI, and photographs of Plaintiff and

Class Members in states of undress are highly offensive to a reasonable person and not a legitimate concern to the public.

It is clear from the facts as alleged, that Plaintiff will have a high likelihood of success on the merits and as such this factor weighs in favor of granting the preliminary injunction sought.

V. ENJOINING DEFENDANT TO MEET THE RANSOM DEMANDS IS REASONABLY SUITED TO ABATE THE OFFENDING ACTIVITY

The fifth factor the Court should consider is whether the injunction is reasonably suited to abate the offending activity. *Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mountain*, 573 Pa. at 647. Pennsylvania courts have found a range of injunctions to be reasonably suited to abating offending activity. In *SEIU Healthcare Pennsylvania v. Commonwealth*, the Supreme Court of Pennsylvania reversed the order of the Commonwealth Court who denied a preliminary injunction to prevent the closure of twenty-six State Health Centers and the subsequent furlough of nurse consultants employed at the State Health Centers. 104 A.3d 495 (Pa. 2014). Regarding whether the injunction was reasonably suited, the Court found that its “issuance of a preliminary injunction instructing the Commonwealth to cease reducing the number of Centers, reestablish Centers in counties in which they have been unlawfully closed, cease reducing the level of public health services, and restore the level of public health services to that which existed on July 1, 1995, is reasonably tailored to abate the Executive Branch's offending conduct.” *Id.* at 509. *See also Kessler v. Broder*, 851 A.2d 944 (Pa. Super. Ct. 2004) (finding that a preliminary injunction requiring majority shareholders of radiology corporations to allocate one-third of the MRI reads to minority shareholders to be reasonably suited).

“Pennsylvania courts sitting in equity have jurisdiction to prevent the continuance of acts prejudicial to the interest of individual rights....” *The York Group, Inc. v. Yorktowne Caskets, Inc.*, 924 A.2d 1234, 1244 (Pa. Super. Ct. 2007). In this case, that is exactly what the injunction

will do. By requiring the Defendants to pay the ransom, this Court would be preventing the further release of Plaintiff and Class Members PHI and PII, including nude images.

Payment of the ransom demand is reasonably suited to abate the threat of further dissemination of PHI and PII because it is the only action suited to abate the threat. Any additional security measures taken by LVHN would simply come too late as ALPHV already has Plaintiff's and Class Members' PHI and PII.

VI. GRANTING THIS INJUNCTION WILL NOT HARM THE PUBLIC INTEREST

Finally, the Court must consider whether the public interest will be harmed if the injunction is granted. *Summit Towne Ctr., Inc. v. Shoe Show of Rocky Mountain*, 573 Pa. at 647. Here, there is no harm to the public interest if the injunction is granted. The protection of PHI and PPI is in everyone's best interest and requiring healthcare providers to put patient privacy above its own financial interest is in the public interest. This injunction is not likely to harm the public interest. Rather this injunction, requiring LVHN to restore the status quo by protecting patient PHI and PII, would protect, rather than harm the public. *See SEIU Healthcare Pennsylvania v. Com.*, 104 A.3d 495, 509 (Pa. 2014).

VII. LVHN SHOULD BE ORDERED TO COMPLY WITH THE DATA BREACH ACT

Despite hundreds, if not thousands of victims, there is no indication that LVHN has sent the requisite notices to those impacted. The Data Breach Act states as follows:

An entity that maintains, stores or manages computerized data that includes personal information ***shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.*** Except as provided in section 41 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, ***the notice shall be made without unreasonable delay.*** For the

purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

73 P.S. § 2303 (emphasis added).

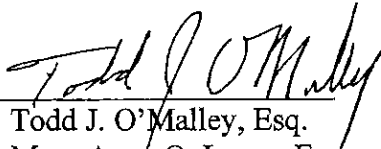
LVHN has been aware of the breach since as early as February 6, 2023. Yet, for some unknown reason, it has not acted to notify the hundreds, if not thousands, of victims so they can take steps to safeguard their privacy. The Court, as part of the injunction, should order LVHN to provide notice immediately.

CONCLUSION

Plaintiff and Class Members have met their burden to prove the need for a preliminary injunction without a hearing. Accordingly, Plaintiff and Class Members respectfully request that the court grant their motion.

Dated: April __, 2023

By: _____


Todd J. O'Malley, Esq.

Mary Anne O. Lucas, Esq.

O'MALLEY & LANGAN

201 Franklin Avenue

Scranton, PA 18503

Tel: (570) 344-2667

Fax: (570) 344-6199

tomalley@omalleylangan.com

mlucas@omalleylangan.com

Simon B. Paris, Esq.

Patrick Howard, Esq. (PA ID #88572)

SALTZ, MONGELUZZI, & BENDESKY, P.C.

1650 Market Street, 52nd Floor

Philadelphia, PA 19103

Tel: (215) 496-8282

Fax: (215) 496-0999

phoward@smbb.com

**IN THE COURT OF COMMON PLEAS
FOR LACKAWANNA COUNTY**

Jane Doe,

Court File No.: 23-CV-1149

*Individually and on behalf of all others
similarly situated,*

Plaintiff,

**[PROPOSED] ORDER GRANTING
PLAINTIFF DOE'S MOTION AND
FOR A PRELIMINARY
INJUNCTION WITHOUT
HEARING**

vs.

Lehigh Valley Health Network, Inc.

Defendant.

AND NOW this ____ day of _____, 2023, pursuant to Pa. R. Civ. P. 1531, the Court having considered Plaintiff's Motion and Incorporated Memorandum of Law, any response thereto, and Reply, if any, the Court hereby GRANTS Plaintiff's Motion for an Injunction Without a Hearing. Defendant, Lehigh Valley Health Network, Inc., is HEREBY ORDERED as follows:

- (1) LVHN within twenty (20) days shall take all steps necessary to prevent the release of additional private, personal and sensitive data onto the dark web of its patients as well as current and former employees. Those steps include, but are not limited to, satisfying the ransom demands of the data hackers; and
- (2) Within (10) days of this Order, provide notice to those reasonably suspected to have been victims of the data breach, including patients, as well as current and former employees. Upon completion, LVHN shall supply this Court with a certification that the notice has been provided in compliance with the Data Breach Act.

IT IS SO ORDERED:

J.